STRATEGY RESEARCH PROJECT

THE YEAR 2000 PROBLEM: CATALYST OR CATACLYSM FOR FUTURE INFORMATION OPERATIONS?

BY

LIEUTENANT COLONEL KEVIN J. GREANEY
United States Army

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1997
U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

DISTRIBUTION STATEMENT A:
Approved for public release. Distribution is unlimited.

THE YEAR 2000 PROBLEM: CATALYST OR CATACLYSM FOR FUTURE INFORMATION OPERATIONS?

by

LTC Kevin J. Greaney

Dr. Robert M. Murphy
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
Carlisle Barracks, Pennsylvania

ABSTRACT

AUTHOR: Kevin J. Greaney (LTC), USA

TITLE: The Year 2000 Problem: Catalyst or Cataclysm For Future Information Operations?

FORMAT: Strategy Research Project

DATE: 26 Mar 1997 PAGES: 27 CLASSIFICATION: Unclassified

The Year 2000 problem centers around how many information systems compute date math problems. In essence, computers affected by the problem use only two digits of the year instead of four when performing date math. This worked well in the last part of the 1900s and saved valuable computer storage space. It will cause problems after the year 2000 and may cause computer failure in one of three ways. The computer system may reject legitimate entries, simply not run, or compute erroneous results. This study explores the Year 2000 problem as the nation's most dangerous, near-term information problem. A second significant theme argues the outdated information technology model is flawed and unsuitable for resolving the problem. The research also reviews the critical information technology issues affecting any potential Year 2000 solution and links the problem and the underlying model to illustrate the shortfalls. Furthermore, the problem may have a negative impact on the information operation doctrine evolving in the Force XXI Advanced Warfighting Experiments and delay deployment of a future Army Vision 2010 force and the Army After Next.

TABLE OF CONTENTS

INTRODUCTION

Information technology is a key element in supporting our national well-being, and is a foundation for our nation's prosperity.[1] Today, the "information superhighway" or National Information Infrastructure, is an initiative for establishing an internetted global information society that engages more nations and enlarges the worldwide economy for the 21st century.[2] Information technology is now a strategic U.S. industry, a foundation for economic growth and an element of national power.[3]

Information technology has also significantly changed the military element of national power. In Operation Desert Storm the world watched on Cable News Network as a US and Coalition force decisively defeated the Iraqi military using an overwhelming information technology. It is also the future cornerstone of Joint Vision 2010; a military strategy focused on achieving information superiority.[4] Today, the Force XXI process integrates information as the essential foundation for future knowledge-based warfare as it develops an information operation doctrine that supports the future Army Vision 2010 strategy.[5]

However, the Information Age has also spawned a host of new, non-traditional information operation threats poised to strike at the National Information Infrastructure. These threats include hackers, viruses and a new breed of sophisticated Cyberspace thieves preying on electronic commerce.[6] There are also other challenges. The 1996 Defense Science Task Force on Information Warfare-Defense report critically stated "we have built our economy and our military on a technology foundation that we do not control and which, at least at the fine detail level, we do not understand."[7]

The author contends there are two other major information technology problems. First, the Year 2000 problem is the nation's most dangerous, near-term, information problem.[8] Second, the current information technology model no longer supports Information Age requirements. This model has also produced a legacy of inefficient, inaccurate, and vulnerable information systems that are too costly to maintain and ill-suited for an Information Age Army. These two problems have potentially serious implications, and present a complex management challenge for the Army. In the long term they could derail the Force XXI, Army Vision 2010, and the Army After Next initiatives.

This paper provides a course of action and required resources for solving the Year 2000 problem and provides the "ways, means, and ends" for developing a near-term information operation capability.[9] It also reviews the critical information technology issues affecting any Year 2000 solution. Finally, it provides recommendations for countering the Year 2000 problem and replacing the current information technology model with one that will support Army Vision 2010 objectives.

THE YEAR 2000 PROBLEM

BACKGROUND. Private and public sector awareness and concern for the Year 2000 problems have grown significantly in the past year. Recent Congressional hearings on the Year 2000 problem included testimony from government, private sector and information technology witnesses.[10] These Congressional witnesses identified the systemic issues with information systems that store the value of the year in a two-digit value instead of the complete four-digit date--for example, 97 for 1997.

A simple math problem illustrates the Year 2000 problem. The problem subtracts twenty years from 2017 resulting in the correct answer of 1997. The Year 2000-affected computers using only two digits, instead of four, will subtract twenty from seventeen for an answer of minus three. There is also another major problem; the next millennium in the year 2000 is a special leap year for correcting the Gregorian calendar. This event only occurs at a four hundred year interval, so the logic in the computer program must factor it correctly.[11] Furthermore, the Year 2000 problem is widespread and may exist on any type of computer-based information system that performs date math. As a result a computer system could fail in three possible ways. It may reject legitimate entries, simply not run, or compute erroneous results.[12]

SCOPE. This problem may affect all levels of the national information infrastructure, including Federal, state, and local governments as well as private sector systems. The problem is ubiquitous, existing in personal computers, and even in such utility systems as traffic lights, security or environmental control systems.[13] It also affects the Department of Defense (DoD) Command, Control, Computers, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) Systems, embedded weapon systems, and business information systems.[14] Unchecked or

mismanaged this problem jeopardizes the essential information operation elements of Joint Vision 2010, information supremacy and dominant battlefield awareness.[15]

In essence, the problem potentially affects millions of lines of computer programming code. The widely publicized estimate for correcting the worldwide Year 2000 problem is $300-600 billion dollars.[16] This rough figure represents only the estimated amount for making existing information systems Year 2000-compliant, with no additional functionality or capability. It does not include any estimates for rectifying first- or second-order effects of the problem, such as going out of business or litigation.[17] The estimated total US cost for solving the problem is approximately $50-75 billion in which the federal government's projected cost is $25 billion or more.[18]

The Social Security Administration has eight years of actual experience on the problem, and is one of the lead government agencies in this effort. The agency expects completion of the $30 million project on 31 December 1998, with one year planned for testing.[19] In the private sector, Allstate, the nation's second largest insurance company, will spend at least $40 million on the problem.[20] Moreover, the lessons-learned from organizations working the problem is that the Year 2000 conversion effort is often larger than envisioned, and costs more than originally estimated.[21] Since many other organizations are just becoming aware of the problem, the scope of the Year 2000 problem for most worldwide organizations is still largely undefined.

The Office of Management and Budget confirmed the Year 2000 problem is "indeed substantial and potentially very serious."[22] Unfortunately, until recently, the issue could not compete with tangible, non-technical problems. The vexing technical aspects, immense scope, and cost projections caused an understandable sense of denial by management.[23] For many years it was much easier rationalizing a technology breakthrough would inexpensively resolve the problem. It is now clear there is no "silver bullet" solution, and the problem has a fixed deadline.[24] The General Accounting Office recently placed the Year 2000 problem on the list of "high risk" programs.[25] These programs are high risk because of the clear potential for fraud, waste, abuse and mismanagement; or there is a serious problem in meeting cost, performance or schedule objectives.

A POTENTIAL THREAT. The DoD Director of Defense Research and Development tasked the MITRE Corporation for a quick assessment of the Year 2000 problem in DoD computer systems, and a validation of the size and scope. The report confirmed the problem's factual basis and made several recommendations, including analysis and testing of all DoD systems, "to avoid potentially disastrous consequences."[26] The DoD Assistant Secretary for Defense, Command, Control, Communications and Intelligence considers Year 2000 to be a serious problem, and stated that "we are treating it much as we would a computer virus...[with] catastrophic consequences should it happen during a...national security crisis."[27] His Deputy Assistant Secretary is also on record as stating, "The Year 2000 problem...is both real and serious,...[and] is a management problem, the magnitude and complexity that we have never before faced."[28]

The Year 2000 problem is a new type of information operation threat. No enemy will wade ashore and no bombs will fall on American cities. The danger comes from within the nation's information systems itself. However, the damage may be more extensive than any foreign attack on the nation. The Year 2000 problem, growing for over thirty years, is a digital "fifth column." This massive problem may cripple the nation's computer information systems; the emerging national information center of gravity.[29] Furthermore, potential foes know the time of this potential window of vulnerability.

The President recently signed a major policy directive, Executive Order 13010, Critical Infrastructure Protection setting the groundwork to prepare the nation against this new type of threat. It established a President's Commission to "recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and ensuring their continued operation."[30] This action was in part influenced by the National Defense Authorization Act for Fiscal Year 1997. It required the President's report to Congress "setting forth the national policy on protecting the national information infrastructure against strategic attacks."[31]

The 1996 Defense Science Board Task Force on Information Warfare-Defense recommended over fifty actions for DoD's preparation for this new type of warfare. It included the following statement: "In the information age as in the nuclear age, *deter* is the first line of defense....This deterrence must include an expression of national will as

expressed in law and conduct, a declaratory policy relative to consequences of an information warfare attack against the United States."[32] The Task Force also recommended reallocating approximately $3 billion over the next five years for implementing the needed actions.[33]

From a strategic planning perspective an understanding of the Year 2000 problem requires a shift from the Industrial Age force-on-force model to an Information Age capabilities-based model. This presents strategic planners with a radical change from a known, well-defined enemy during the Cold War. Today, planners must develop strategies against a plethora of non-traditional threats engaged in asymmetrical, offensive information operations against US national interests and power.[34]

CRITICAL INFORMATION TECHNOLOGY MODEL ISSUES

The Year 2000 is not the only critical information technology issue facing the Army today. A critical analysis of the current Army information technology model reveals several other significant shortcomings in the "as is" information technology environment that will have an adverse impact on any plan to resolve the problem. Some of these major problems are: *data integration, data accuracy, data overload, horizontal and vertical integration, an outmoded Industrial Age information technology model, and security.*

DATA INTEGRATION PROBLEMS. Data integration is a significant operational problem today. In Bosnia the commander needs a "fused real-time, true picture" that is flexible enough for his changing critical information requirements.[35] According to the deputy commander of U.S. Army Europe, the ground-truth was, "What I had was a lot of stuff, not all integrated."[36]

Prairie Warrior 96, an "advanced warfighting experiment," demonstrated the beginnings of integration and interoperability with a limited set of task force messages. It was a positive step toward "common information sharing through database queries."[37] However, it also found that "more effort must be placed on database continuity...from target C4I system through...interfaces to the JTC."[38] Observations from Prairie Warrior 96 included: "training must include adherence to database standards and full C4I system integration."[39]

The 4th Infantry Division at Ft. Hood is developing the Division XXI redesign for total battlefield awareness. However, integration is still an issue. The task force fixed all "warstoppers" identified in early September 1996, except one, the "vertical information flow from appliqué to battalion."[40] The consensus from platoon lane test evaluations stated: "situation awareness works, but not often; electronic overlays do not work and overall the system is not ready for the National Training Center."[41]

DATA ACCURACY PROBLEMS. The Army has also experienced problems in *data accuracy*. In the personnel arena, this has adversely affected service to soldiers and critical decision processes. The Deputy Chief of Staff for Personnel established a "Data Accuracy Task Force" and charged it with correcting the situation. The proposed solution is a two-phased migration plan for a Total Army personnel information architecture. This includes the "creation of an Army personnel database -- a single, integrated multi-component database" that will provide accurate, real-time visibility of all Army military human resources in both peace and war.[42]

In a logistic case study, the Integrated Combat Service Support System is being designed as the logistic management information system for Force XXI. This project will integrate several logistic Standard Army Management Information Systems. It will be the "Army's single, seamless, integrated, and interactive combat service support automation and information management system, with true integration of the data."[43]

The cited data accuracy and data integrity examples are pervasive in many types of information systems. The case studies from the personnel and logistics domains indicate a systemic type of problem. Both of the organizations have selected a limited, vertical, and functionally oriented scope for resolving the issue. In neither case is there any indication of a business process reengineering effort or an objective of horizontally integrating the new systems across the Army in support of Army Vision 2010.[44]

INFORMATION OVERLOAD. Another issue, closely related to data problems is *information overload.* An emerging advanced warfighting experiment insight reveals the system cannot overwhelm leaders with data. Therefore, at all levels, commanders and staffs must develop an ability for "information assessment...the ability for selecting and extracting vital information from the great mass of useless information provided," or data will overwhelm them.[45]

HORIZONTAL AND VERTICAL INTEGRATION. Data accuracy issues, data integrity problems, and information overload are all indicators of a systemic horizontal and vertical integration problem. Several organizations in the Training and Doctrine Command and the materiel development community throughout the Army today perform horizontal and vertical integration.[46] Within their respective domains, these organizations perform a critical function; although they have a limited domain expertise, level of responsibility, organizational focus, and resources. No one organization has the complete capability for horizontal and vertical integration scope of information for the entire Army. For the most part, the current horizontal integration process for information has failed. Congressional hearings, Government Accounting Office, and Office of Management and Budget agencies have identified and documented this shortfall in several critical reports.[47]

AN OUTMODED INDUSTRIAL AGE INFORMATION TECHNOLOGY MODEL. The issues with data accuracy, data integrity, information overload, and horizontal integration are only part of the information technology model problem confronting the Army today. The high cost of information technology and the existing low state of software development productivity indicate the Army is not getting a good return on investment for its money. The new Secretary of Defense, William S. Cohen, is highly critical of government management of information technology. In 1994 he provided a scathing report, "Computer Chaos: Billions Wasted Buying Federal Computer Systems." The report criticized the Federal Government's weak oversight and failure to give the taxpayers a good value for $200 billion expended over the past ten years.[48]

Furthermore, in spite of this large investment, government "operations continue to be hampered by inaccurate data and inadequate systems."[49] The Cohen report also cited poor process design and data management processes. It recommended the government make needed process and business changes before developing automated solutions to improve its operations. The report continued by recommending the saving of billions of dollars by first reforming administrative practices. [50]

Cohen's report also found DoD financial systems produced inaccurate and unreliable data was critical of DoD's operation of 161 different major accounting systems running on outmoded computer systems.[51] In addition, the information DoD needs is in many cases unavailable, incomplete, or in an unusable format.[52] The lack of standardized

data structures across systems resulted in database queries for different systems providing multiple answers. The Cohen report asserted, "DoD's failure to modernize its computer systems will have a serious effect on military readiness and DoD's ability to purchase major weapon systems."[53]

In an era of tight budgets, information technology numbers are huge. Annual federal information technology expenditures account for almost 5 percent of all federal discretionary spending and 12.5 percent of government procurement of goods and services.[54] Furthermore, the DoD spends 37 percent of the government's computer budget, the largest federal purchaser of information technology.[55]

Not only is the scope of known DoD information technology investments staggering; the DoD is not sure how much it spends on information technology. Of an estimated $25 to $42 billion reported annually by DoD on computer systems, less than $7 billion of this total is for hardware.[56] In addition, the DoD has estimated that it spends an additional $24 to 32 billion annually for software embedded in weapon systems.[57] It is obvious software has become the major cost, performance, and schedule driver for DoD.

Other findings identified significant first- and second-order problems. Some examples of these systemic types of problems illustrate the enormous cost borne by the taxpayer for mistakes that provide no benefit to the DoD. In one instance, the DoD bought $30 billion of spare parts it did not need. During one accounting period DoD accrued over $41 billion in payments it could not match up with invoices.[58] In an another case, the DoD in one six-month period, experienced $751 million in returned DoD contractor overpayments.[59]

The situation from a cost, performance, and schedule perspective is also negative. Failures or major defects in large information systems can have very significant economical impact. According to Capers Jones, a noted software industry analyst, the number of defects in software as measured by function points, increases exponentially and becomes more significant in larger systems.[60] Function points have replaced lines of codes as a commonly accepted measurement of sizing and costing information systems. Many nations have a skilled workforce that can develop software between $125 and $250 per function point, while the cost is $1,000 per function point in the United States.[61]

Similarly, as software systems have become larger, the ability for managing these systems has not kept pace. Development costs continue rising dramatically while overall software development productivity has not improved. The Software Engineering Institute in the past ten years has developed a widely accepted software process improvement model for evaluating capabilities of software developers, the Capability Maturity Model. The effort has not achieved the desired results. In a review of the 379 participating organizations that have process improvement programs in place, 73 percent rate no higher than the lowest level of productivity.[62] Productivity is a significant issue, since the DoD now depends on outsourcing most software development work into the private sector.[63] The comparatively high cost of US software developers and their relatively low productivity on large system development forecasts a daunting challenge for resolving Year 2000 problems.

There are other significant issues for achieving the goal of Year 2000 compliancy. As the millennium year draws nearer, there will be stiffer competition and greater demand from the public and private sectors for scarce programmer resources. The well-documented limitations of the DoD acquisition system for acquiring timely services and materials may further complicate the solution of the Year 2000 problem.[64] Compounding this situation as demand outpaces the supply of domestic software developers, there is the potential for contractors doing work overseas cheaper, with foreign nationals. In compressing an effort of this scope into a very short timeline, the situation also poses a potential security threat. The immediate emphasis will be on fixing the problem; and not integrating information security safeguards that will prevent programmers from inserting vulnerabilities into the software code.

SECURITY. Information security, information assurance and computer network attacks have been a systemic shortfall of DoD information systems and other federal agencies.[65] The shortage of technically qualified personnel compounds this issue.[66] This includes trained and certified system administrators and technical oversight at the government-enterprise level. There are many vulnerabilities in the current federal information systems. The Government Accounting Office (GAO) reports the DoD may have experienced 250,000 computer network attacks in 1995.[67] Of these attacks approximately 64 percent of successfully resulted in unauthorized access, and DoD

detected very few.[68] The GAO has concluded that in spite of the criticality of federal information systems, "they are not being adequately protected" from unauthorized access.[69] The GAO has documented this shortfall in over 30 reports.[70] In view of the risks to national security if this condition continues, the GAO placed information security on the high-risk list of programs needing special oversight.

THE ARMY PROJECT CHANGE OF CENTURY PLAN. In the aforementioned information environment, the Army recently developed a Year 2000 plan for repairing information systems with the Year 2000 problem.[71]. Resources will initially come from internally reprogrammed sources, although DoD submitted estimates of an additional $970 million for the Year 2000 problem with the President's Fiscal Year 98 budget.[72] In the resource-constrained environment the emphasis will be on mission-critical systems.

However, the plan's most immediate challenge may be in the testing community. The testing community has only limited cost estimates for a small percentage of affected DoD systems. The Testing and Evaluation Joint Program Office currently estimates a cost of $22.5 million for fixing its own five hundred internal automated systems needing Year 2000 compliance.[73] Furthermore, the testing community has not scheduled critical customer tests and there is no identified funding stream for Year 2000 testing.[74] The lack of time, limited available testing resources, and the scale of required synchronization efforts are significant impediments for solving the Year 2000 problem in time.[75]

END, WAYS, AND MEANS FOR A NEW INFORMATION MODEL

Any solution for solving the Year 2000 problem and developing an Army Vision 2010 information operation capability requires the application of an Information Age ends, ways, and means. The application of these criteria provides an alternative for solving the Year 2000 problem by "organizing around information."[76] The following three models provide a theoretical framework for developing a reference model upon which to build the physical ends, ways and means.

ENDS. Information is the core resource of military effectiveness and the foundation for information supremacy.[77] The concurrently evolving threads of parallel activity, such as the Force XXI advanced warfighting process, comprise the environment of this new model. However, dealing with this new model will take a complete change of

cultural attitudes and runs counter to a well-established requirement and acquisition system.

In today's Industrial Age model there is more emphasis on hardware technology, the speed of networks moving data, and the capacity for storing data; than the underlying content and data integrity of the information.[78] Unfortunately, the current Industrial Age model of constantly replacing information systems with faster computers and networks has failed in the primary purpose of providing "decisionable information."[79]

The first order of business is understanding the full meaning of information. The Cognitive Hierarchy Model, prescribed in Joint Pub 6.0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations* and Army Field Manual 100-6, *Information Operations*, defines the processes that transform data into information and ultimately into understanding. This reference model also prescribes six information quality criteria for commanders and planners: accuracy, relevance, timeliness, usability, completeness, and precision.[80] In a minor difference, Joint Pub 6.0 defines precision as brevity and adds a seventh criterion, security.[81]

Field Manual 100-6 also groups the information quality criteria into three priority groups: accurate and relevant information, timely and usable information, and complete and precise information.[82] It then applies the following heuristics, stating "incomplete or imprecise information is better than none at all; untimely or unusable information is the same as none at all; [and] inaccurate or irrelevant information is worse than none at all."[83] It appears that a solution for the data accuracy, data integrity and data overload problems in the current information model starts with the lowest level of the Cognitive Hierarchy, data. The solution would then step up the Cognitive Hierarchy model; a sequential model, consisting of four layers, with each one building on the foundation layer of data.

MEANS. A second point worth reviewing is the population involved in the process as the Army transitions into the new warfare dimension of information operations. The current model worked well for developing major weapon systems over time and allowed for the balancing of current operations with future modernization. It has not worked well for information systems. Information is no longer just a business decision or a technical problem as we view it today. Information superiority is central to

the way the Army will fight and defend the nation in the 21st century.[84] Commanders, warfighters, and logisticians should actively participate in all activities of the model.

In a second model, Dr. A.H. Maslow's seminal work, the Hierarchy of Needs models the motivation of people in the workplace. This model closely represents the most critical element of an Information Age Army, the individual soldier. It describes the five basic needs all soldiers face, organized into successive tiers; survival, safety, love esteem and the highest need, self-actualization.[85] When a soldier meets an existing need, they identify a higher one. Although a previous need does not require complete satisfaction before moving on to the next one, the emergence of these higher needs follows to a certain extent, from the satisfaction of the previous level(s).[86] The Force XXI advanced warfighting experiment is the Army's initial corporate effort of systematically applying information doctrine to its most critical mission, warfighting. The advanced warfighting experiment process inserts the warfighter at the lowest level of the hierarchy, totally immersing him in the process of assimilating the strength's and weaknesses of information technology. As the process matures soldiers will develop a common reference set of Information Age tactics, techniques, and procedures and advance up the hierarchy. Similar to the Cognitive Hierarchy, this model is also sequential; consisting of five layers, with each one building on the previous one.

WAYS. The Capability Maturity Model is the third model reviewed. The Software Engineering Institute developed it after decades of frustration over the lack of productivity. This model measures the maturity of organizations attempting to develop the automated processes that transform the data into information on the Cognitive Hierarchy Model. The critical issue it addresses is the fundamental inability of software development organizations to manage the software development process. The five layers of process maturity ranging from low to high: initial, repeatable, defined, managed, and optimizing; provide a scale for measuring the organization's process maturity.[87] This model links the previous models and requires commensurate progress in both before developing quality software. The warfighter defines the critical data requirements and the processes that wicker the great morass of useless data into "decisionable information." Furthermore, the warfighter must grow and evolve with the process or fail to reach the

highest level of the hierarchy. Like Maslow's model it provides a five-level framework, with each level providing a foundation for continuous process improvement.

INFORMATION SUPERIORITY CORRELATION MODEL. A new information model borrows heavily from the three reference models. My hypothesis suggests there is a correlation among the three models that I call the *Information Superiority Correlation Model*, for the following reasons. First, all three models share the same construct and have similar rule sets. Second, they all prescribe a hierarchical, sequential advancement process dependent on satisfying the criteria for the current level. Third, a setback in any of the previous tiers delays or reverses advancement in the model. These models reflect what I consider are the three essential components of the new information technology model; the end, ways and means of incorporating the warfighter the data and the processes that mold the data into information. Finally, in the Cognitive Hierarchy model this hypothesis infers that without quality criteria for data at the lowest level and valid processes applied to the data, information -- is unattainable.

Information Superiority Correlation Model

"To Be" State

Maslow's Hierarchy of Needs	Capability Maturity Model	Cognitive Hierarchy
Self Actualization **Egoistic Needs Satisfied**	Optimized **Continuously Improving Process**	*Wisdom*
Esteem **Social Needs Satisfied**	Managed **Predictable Process**	Understand **Judgment**
Love **Protection Needs Satisfied**	Defined **Standard Consistent Process**	Knowledge **Cognition**
Safety **Survival Needs Satisfied**	Repeatable **Disciplined Process**	Information **Processing**
Survival **"As Is" State**	Initial	Data **Figure 1**

CONCLUSION

Any Year 2000 solution predicated on the current information technology model will fail. The current information technology model evolved over time with no master plan for guidance. The preponderance of evidence indicates it is costly, ineffective and flawed. In addition, the current Industrial Age requirement definition and material development processes supporting the information technology model are ill-suited for an evolving Information Age model.

The Army should reexamine the basic model of how it will develop the information technology for achieving Army Vision 2010. The campaign plan for achieving the Army Vision 2010 assumes the Army's "as-is" information technology position is secure. This assumption is false. The failure of properly identifying and addressing all current information technology model issues early in the Year 2000 planning process, will undermine any future doctrine or strategy based on information operations. This will have an immediate adverse impact on solving the Year 2000 problem and meeting future Army Vision 2010 objectives. Furthermore, any model must define the strategic ends, ways and means for developing an information operations capability.

Finally, any solution that under-estimates the Year 2000 problem could result in the reallocation of significant fiscal resources from future Army force structure, readiness and modernization accounts. In the projected austere budgeting environment this may place Army missions at considerable risk. There is also a potentially grave danger for the national security if mission-critical systems become significantly degraded by the Year 2000 effect simultaneously at a time known by any potential adversary.

RECOMMENDATIONS

The recommended model for achieving the "to be" state incorporates the tenets of the Information Superiority Correlation Model, is architecture-based, accountability driven, and executed in a distributed methodology by empowered information operators. Joint Vision 2010 and Army Vision 2010 are the conceptual templates for the "to be" state. They call for an increased access to information, and "improvements in the speed

and accuracy of prioritizing and transferring of data."[88] Future joint military operations will also require information superiority, the strategic information operation *ends*.

The methodology for evolving the vision into reality is through the DoD Joint Technical Architecture and Army Technical Architecture. This physically implements the strategic information model *ways*. These key documents also provide the ways for providing an enterprise-wide, horizontally and vertically integrated Year 2000 solution. They form the foundation around an interrelated set of "building blocks": an Operational Architecture, a System Architecture, and a Technical Architecture. The Operational Architecture is the total aggregation of missions, functions, tasks, information rules, and business rules that defines the type of information required for complete horizontal integration. It also defines the frequency of exchange and the tasks supported by these information changes.[89] The Operational Architecture is a critical component for resolving the Year 2000 problem and achieving Army Vision 2010.

However, the architectures in of themselves will not resolve the Year 2000 problem. There is a second required element of the model. At the DoD level, Dr. Paul Kaminski identified a need for: "Readiness measures...to include overall management of information [and] a system of measures with which to gauge our readiness in this area....Once established, these readiness measures should be evaluated, monitored, and reported periodically."[90] At the Army level, the Director of Army Artificial Intelligence stated, "A clear big picture vision within DoD is missing."[91]

The "big picture" is an information equivalent to the Unit Status Report--an Army Information Status Report. In the new information model, Joint Pub 6.0 and Field Manual 100-6 provide the seven information quality criteria and three priorities for the data requirements defined by the Operational Architecture. An Army Information Status Report would ideally provide service information for a Joint Information Status Report. The objectives of the Information Status Report are: (1) provide the warfighter with "decisionable information;" (2) improve the information security posture of Army information systems; (3) give the Army an accurate enterprise information status; (4) develop a quantifiable method of supporting and defending information systems resource decisions; (5) affix responsibility for processes and data; (6) provide a firm foundation for the "systems of systems"; (7) integrate horizontally and vertically at the enterprise

level; and (9) supports bandwidth requirements. The Information Status Report provides a critical part of the foundation for improving data accuracy and integrity, while reducing information overload.

The third issue is who, how, when, and where will this capability come from in today's constrained environment. The Army Officer Personnel Management XXI Task Force has developed a future professional development model, that includes a career field in information operation.[92] Dr. Kaminski's white paper also addressed the personnel shortcomings and lack of a career path for personnel who "will manage our critical information warfighting functions....What is needed now is an individual with hybrid qualities, a combination of intelligence officer, an operations officer, a C4 expert, and a logistician."[93] A recent article on knowledge-based warfare gave additional insights on information operation roles stating: "C4ISR is a combat function of the information age....C4ISR personnel, organizations, and processes-traditionally regarded as combat support-must now be defined as integral to combat....Operations will absorb many functions we associate with intelligence."[94] Another article called for the establishment of an Information Corps that would "create common doctrine for the diverse requirements of information warriors...facilitate liaison among civilian information agencies....[and] obviate the need for the services to integrate data systems because standardization would exist from the outset."[95] This capability would provide the strategic information *means.*

An empowered information operation corps would provide the Army with a capability for simultaneous, synchronized, and distributed information operation -- organized around information.[96] Similar to the JCS J-3 model, the DCSOPS would be the operational proponent and integrate this capability within the Army, ensuring unity of effort for Army information operations. An Information Status Report and an Army information operation corps would provide the strategic information operation means. This embryonic information operation capability would evolve into a corps capable of achieving the goals of focused logistics and information supremacy.

However, the Year 2000 problem requires a near-term solution. An option available today is the creation of an information operation officer corps from the Army functional area 53 -- system automation officer population. This option would also include selected officers with artificial intelligence skills from any branch. It takes

advantage of a corps of officers with significant technical expertise who are now in TDA, TOE, Joint, and DoD positions worldwide. It also has representation by officers in most branches and year groups.[97] This course of action requires no additional force structure and would provide a basic corps of information operators, now. Other specialties, functional areas, or branches could augment the information operation corps. Near-term this option provides the Army with a contingency corps of officers for solving the Year 2000 problem.

The Army would implement the last, critical step of the model -- the accountability feedback loop -- after developing, testing, and implementing the Information Status Report. Individuals assigned a specific responsibility in the Information Status Report process would submit measurable indicators of their performance in this area on their Officer Evaluation Report support form. This would happen at all levels down to the data element proponent. This procedure would facilitate the senior proponent's integrated oversight responsibility of the budget, requirement, acquisition, and information systems. Using this accountability-based model would vastly improve the Army's capability for enterprise-wide horizontal and vertical information integration.

Finally, the DoD should model the degradation or loss of mission critical systems and develop contingency plans. The DoD should then analyze and assess the risks of potential first- and second-order Year 2000 problems for the nation. The Army in conjunction with interagency working groups, should review and revalidate domestic recovery and reconstitution plans. This working group must plan for a worst-case scenario that critically affects all the centers of national power--economical, political, psychological and military--simultaneously.

As significant as the Year 2000 problem will be, it represents a tactical defensive information operation; and in a sense, a large-scale, digital combat training center opportunity. The Army must apply the proper end, ways and means for developing a defensive information operation capability against the threat. If we fail, future military historians may call the Year 2000 problem a digital version of a "Task Force Smith."[98] This alternative future could be far more devastating than any conventional defeat. In a

worst case scenario, the Year 2000 problem may stretch and tear at the fabric of all American national powers

ENDNOTES

[1] National Defense University, Strategic Assessment 1996, (Washington: National Defense University Press, 1996), 78-80.

[2] United States General Accounting Office, Information Superhighway: An Overview of Technology Challenges, (Washington: United States General Accounting Office, January 1995), 10.

[3] National Defense University, 79-80.

[4] John M. Shalikashvili, Joint Vision 2010 (Washington, DC: The Joint Staff, 1996), 16.

[5] Dennis J. Reimer, Army Vision 2010 (Washington, DC: The Army Staff, 1996), 1.

[6] United States General Accounting Office, 19-24.

[7] Ibid., 2-9.

[8] Congress, House of Representatives, Government Management, Information and Technology Subcommittee of the House Government Reform and Oversight Committee, Holds Hearing on the Year 2000 Problem, 105th Cong., 1st sess., 14 February 1997, 1-7.

[9] Arthur F. Lykke, Jr., "Toward an Understanding of Military Strategy," Military Strategy: Theory and Application, ed. Arthur F. Lykke, Jr. (Carlisle Barracks: 1993), 3.

[10] Ibid., 1-2.

[11] Congressional Research Service Report, "The Year 2000 Computer Challenge," n.d.. <http://infosphere.safb.af.mil/~jwid/fadl/world/crsrpt.htm> 7 January 1997.

[12] Ibid.

[13] Ellen Perlman, "Techno-Terror 2000," September 1996, <http://web.governing.com/governing/92000.html>, 5 December 1996.

[14] Emmett Paige, testimony, "Before the House Committee on Government Reform and Oversight Subcommittee on Government Management, Information and Technology United States House of Representatives," 16 April 1996, <http://www.itpolicy.gsa.gov/mks/yr2000/y216cng1.htm>, 12 January 1997.

[15] Shalikashvili, 13.

[16] Ronald Spear, "1 January 2000 is a Saturday," n.d. <http://www.army.mil/disc4/newslet/vp-96win/yr2000.htm>, 16 December 1996.

[17] Ibid.

[18] Ibid.

[19] Allan Holmes, "Bill Seeks Year 2000 Compliance," n.d., <http:/160.147.68.21:80/army-y2k/articles/bill.htm>, 17 November, 1996.

[20] Lee Gomes, "A Look at Allstate Shows Why Preparing for 2000 Is So Tough", 9 December 1996, <The Wall Street Journal Interactive>, 9 December 1996.

[21] George Munoz, "Computer Challenge," 16 April 1996, <http://www.itpolicy.gsa..gov/mks/yr2000/y216cng1.htm>, 12 January 1997.

[22] Sally Katzen, testimony, " Statement of Sally Katzen, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget Before the Subcommittee on Technology...U.S. House of Representatives," 10 September 1996, <http://www.itpolicy.gsa.gov/mks/yr2000/katzen.htm>, 12 January 1997.

[23] Ibid.

[24] Ibid.

[25] GAO/HR-97-9 High-Risk Series, "Information Management and Technology," February 1997, <http:/www.gao.gov/highrisk/hr97009.txt>, 13 February 1997.

[26] John Roberts, "Year 2000 Assessment Report Executive Summary," 24 April 1996, <http://www.mitre.org?research/y2k/docs/exec_sum.html>, 18 December 1996.

[27] Paige.

[28] Tony Valletta, "Year 2000 Problem," 2 May 1996, <http://www.itpolicy.gsa.gov/mks/yr2000/y220dmb2.htm>, 12 January, 1997.

[29] The Joint Staff, Doctrine for Joint Operations, Joint Publication 3-0, (Washington: The Joint Staff, 1 February 1995), III-20.

[30] Defense Science Board Task Force, Information Warfare - Defense (IW-D), (Washington: Defense Science Board, November, 1996), preface.

[31] Ibid., ES-3.

[32] Arthur K. Cebrowski, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance (Washington, DC: The Joint Staff, 4 July 1996), 2-59.

[33] Defense Science Board Task Force, 6-33.

[34] Defense Science Board Task Force, 2-2 - 2-4.

[35] LTG Robert Gray, "Full-spectrum Warfare: the Future's Shape", n.d. <http://www.ggordon.mil/OCOS/BM/AC/WINT97/GRAY.HTM>, 21 January 1997.

[36] Ibid.

[37] Thomas E. Brown, "PW 96: Insights and Observations," Military Review (July-August 1996): 16.

[38] Ibid., 21.

[39] Ibid., 21.

[40] Peter Farrell, <Farrellp@carlisle-emh4.army.mill>, "Minutes of Force XXI In Progress Review for Chief of Staff of the Army," 8-10 October 1996." Electronic mail message to Kevin J. Greaney, <greaneyk@carlisle-emh2.army.mil>. 25 October 1996.

[41] Ibid.

[42]C. Willis, "PERSCOM to Remodel Personnel Information System Architecture," n.d. <http://www-prescom.army.mil/gendocs/strategic.htm>, 2 January 1997.

[43] William R. Haugh, "Force XXI Logistic Management Information System Starts," The ViewPoint (Fall 1996): 15.

[44] Department of the Army, Information Operations, U.S. Army Training and Doctrine Command Pamphlet (Fort Monroe, VA: U.S. Army Training and Doctrine Command, August, 1996), 2-13.

[45] Richard A. Chilcoat, Strategic Art: The New Discipline for 21st Century Leaders (Carlisle, PA: U.S. Army War College, 10 October, 1991), 17.

[46] Department of the Army, Information Operations, U.S. Army Training and Doctrine Command Pamphlet (Fort Monroe, VA: U.S. Army Training and Doctrine Command, August, 1996), 2-13.

[47] Congress, Senate, Subcommittee on Oversight of Government, Senate Government Affairs Committee, Computer Chaos: Billions Wasted Buying Federal Computer Systems, report prepared by Senator William S. Cohen. 103d Cong., 2d sess., 1994, <http://ftp.senate.gov:70/0/member/me/cohen/general/computer_chaos>, 4 November 96.

[48] Ibid.

[49] General Accounting Office, Information Technology Investment: Agencies Can Improve Performance, Reduce Costs, and Minimize Risks (Washington: U.S. General Accounting Office, 1996), <http://www.access.gpo.gov/cgi-bin/useftp....i96064.txt&directory=/diskb/wais/data/gao>, 11.

[50] Congress, Senate.

[51] Ibid.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Norm Brown, "Industrial-Strength Management Strategies," n.d. <http://www.stsc.hill.af.mil/www/xt96aug/xt96d08e.html>, 5 January 1997.

[57] General Accounting Office, Information Technology: Best Practices Can Improve Performance and Produce Results (Washington: U.S. General Accounting Office, 26 February 1996), <http://www.access.gpo.gov/cgi-bin/useftp....i96046.txt&directory=/diskb/wais/data/gao>2 November 1996.

[58] Ibid.

[59] Ibid.

[60] Norm Brown.

[61] Ibid.

[62] Ibid.

[63] John P. White, "Outsourcing Stretches DoD Dollars," Defense 96 (Issue 3): 21-23.

[64] National Defense University, 75.

[65] Department of Defense, Information Operations (IO) (U), Department of Defense Directive S-3600.1(Washington: U.S. Department of Defense, 9 December 1996), 1-1.

[66] Government Accounting Office/HR-97-9.

[67] Ibid.

[68] Ibid.

[69] Ibid.

[70] Ibid.

[71] Otto J. Guenther, "U.S. Army Project Change of Century Action Plan," 4 October 1996, <http://160.147.68.21.:80/army-y2kr/army.plan/Revision1/3gPCCsusp4.htm>, 7 January 1997.

[72] U.S. Office of Management and Budget, "Getting Federal Computers Ready for 2000," 6 February 1997, <http://www.comlinks.com/gov/omb2697.htm>, 21 February 1997.

[73] Rod Wilkinson, "The T&E response to the 14 Nov DTSE&E memo (USD)(A&T) Year 2000 Kick-off Meeting) requiring an updated report of anticipated Year 2000 impacts for each functional user," 11 December 1996, < http://140.229.1.16:9000/htdocs/teinfo/y2kstat.htm>, 8 February 1997.

[74] Ibid.

[75] Ibid.

[76] Gordon R. Sullivan and Michael V. Harper, Hope is Not a Method (New York: Times Books, 1996), 163.

[77] Donn A. Starry and Huba Wass de Czege, "How To Change an Army," March 1983 and November 1984 <http://call.mil:1100/call/exfor/specrpt/exsum.htm>, 15 January 1997, 16. Analysis of the Toffler-Brown perspective indicates a need to add the factor of information to the eight "constanst" of the Starry-Wass de Czege paradigm.

[78] Robert D. Steele, "Creating A Smart Nation: Information Strategy, Virtual Intelligence and Information Warfare," Cyberwar: Securit, Strategy, and Conflict in the Information Age, ed. Alan Campen, Douglas Dearth, and R. Thomas Goodden (Fairfax: AFCEA International Press, 1996), 77.

[79] Lawrence A. Casper et al., "Knowledge-Based Warfare: A Security Strategy for the Next Century," Joint Force Quarterly 13 (Autumn 1996): 83.

[80] Department of the Army, Information Operations, Field Manual No. 100-6 (Washington: U.S. Department of the Army, 27 August 1996), 4-1.

[81] The Joint Staff, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations, Joint Pub 6-0 (Washington: U.S. Joint Staff, 30 May 950, I-5.

[82] Department of the Army, 4-1.

[83] Ibid., 4-1.

[84] Dennis J. Reimer, Army Vision 2010 (Washington, DC: The Army Staff, 1996), 2.

[85] Carl Heyel, "Motivation: Maslow's Basic Needs", The Encyclopedia of Management, ed. Carl Heyel (New York: Van Nostrand Rheinhold Company, 1982), 728-729.

[86] Ibid., 728.

[87] Watts Humphrey, Managing the Software Process (n.p.: 1989), <http://ricis/cl.uh.edu/CMM/TR24/tr24_cl.html#C130>, 26 February 1997.

[88] Joint Vision 2010, 16.

[89] Gibert Deckert and Ronald Griffith , Army Technical Architecture, Department of the Army (Washington: U.S. Department of the Army, 30 January 1996), executive summary.

[90] Paul Kaminski, "Information Superiority/Dominant Battlespace Awareness: Some Critical Missing Elements," a white paper, Washington, n.d.

[91] Duard S. Woffinden, "Artificial Intelligence and the Information Interoperability Puzzle," a paper for the 2nd International Workshop on Multimedia Information Systems, West Point, New York, 28 September, 9.

[92] Davis Ohle, "The Director's View," information paper on status of OPMS XXI Task Force, Washington, n.d., <http://www.army.mil/opms/DIRECTOR.HTM>.

[93] Kaminski, 2.

[94] Casper et al., 88.

[95] Ibid., 88.

[96] Sullivan, 161-162.

[97] Earl Rasmussen, "What is a '53'? A Perspective," information paper on Army system automation officers, Washington, n.d., <http://www.sarda.army.mil/dacm/publications/articles/53ptlv4.html>,1.

[98] Gordon Sullivan, "Army Drawdown Chain Teaching Briefing," Washington, 1992.

BIBLIOGRAPHY

Brown, Norm. "Industrial-Strength Management Strategies," n.d. <http://www.stsc.hill.af.mil/www/xt96aug/xt96d08e.html>. 5 January 1997.

Brown, Thomas E. "PW 96: Insights and Observations," Military Review (July-August 1996): 11-22.

Cebrowski, Arthur K. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance . Washington, DC: U.S. The Joint Staff, 4 July 1996.

Chilcoat, Richard A. Strategic Art: The New Discipline for 21st Century Leaders . Carlisle, PA: U.S. Army War College, 1995.

Congress, House of Representatives, Government Management, Information and Technology Subcommittee of the House Government Reform and Oversight Committee. Holds Hearing on the Year 2000 Problem. 105th Cong., 1st sess., 14 February 1997.

Congressional Research Service Report. The Year 2000 Computer Challenge, n.d.. <http://infosphere.safb.af.mil/~jwid/fadl/world/crsrpt.htm>. 7 January 1997.

Decker, Gibert T. and Ronald Griffith. Army Technical Architecture. Washington: U.S. Department of the Army, 30 January 1996.

Defense Science Board Task Force. Information Warfare - Defense (IW-D). Washington: Defense Science Board, November, 1996.

Farrell, Peter. <Farrellp@carlisle-emh4.army.mill>. "Minutes of Force XXI In Progress Review for Chief of Staff of the Army," 8-10 October 1996." Electronic mail message to Kevin J. Greaney, <greaneyk@carlisle-emh2.army.mil>. 25 October 1996.

Gomes, Lee. "A Look at Allstate Shows Why Preparing for 2000 Is So Tough", 9 December 1996. <The Wall Street Journal Interactive>. 9 December 1996.

Gray, Robert. "Full-spectrum Warfare: the Future's Shape", n.d. <http://www.ggordon.mil/OCOS/BM/AC/WINT97/GRAY.HTM>. 21 January 1997.

Guenther, Otto J. "U.S. Army Project Change of Century Action Plan," 4 October 1996. <http://160.147.68.21.:80/army-y2kr/army.plan/Revision1/3gPCCsusp4.htm>. 7 January 1997.

Haugh, William R. "Force XXI Logistic Management Information System Starts." The ViewPoint (Fall 1996): 15.

Humphrey, Watts. Managing the Software Process. 1989. <http://ricis/cl.uh.edu/CMM/TR24/tr24_cl.html#C130>. 26 February 1997.

Heyel, Carl, ed. "Motivation: Maslow's Basic Needs", The Encyclopedia of Management. New York: Van Nostrand Rheinhold Company, 1982.

Holmes, Allan. "Bill Seeks Year 2000 Compliance," n.d. <http:/160.147.68.21:80/army-y2k/articles/bill.htm>. 17 November, 1996.

Katzen, Sally. " Statement of Sally Katzen, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget Before the Subcommittee on Technology...U.S. House of Representatives," 10 September 1996. <http://www.itpolicy.gsa.gov/mks/yr2000/katzen.htm>. 12 January 1997.

Kaminski, Paul. "Information Superiority/Dominant Battlespace Awareness: Some Critical Missing Elements." a White Paper. Washington, n.d.

Lykke, Arthur F. Jr., ed. "Toward an Understanding of Military Strategy," Military Strategy: Theory and Application. Carlisle Barracks, PA: United States Army War College,1993.

Munoz, George. "Computer Challenge," 16 April 1996. <http://www.itpolicy.gsa..gov/mks/yr2000/y216cng1.htm>. 12 January 1997.

National Defense University. Strategic Assessment 1996. Washington: National Defense University Press, 1996.

Ohle, Davis. "The Director's View." Washington, n.d. <http://www.army.mil/opms/DIRECTOR.HTM>. 28 January 1997.

Paige, Emmett. "Before the House Committee on Government Reform and Oversight Subcommittee on Government Management, Information and Technology United States House of Representatives," 16 April 1996. <http://www.itpolicy.gsa.gov/mks/yr2000/y216cng1.htm>. 12 January 1997.

Perlman, Ellen. "Techno-Terror 2000," September 1996. <http://web.governing.com/governing/92000.html>. 5 December 1996.

Rasmussen, Earl. "What is a '53'? A Perspective." Washington, n.d. <http://www.sarda.army.mil/dacm/publications/articles/53ptlv4.html>. 9 December 1996.

Reimer, Dennis J. Army Vision 2010. Washington, DC: The Army Staff, 1996.

Roberts, John. "Year 2000 Assessment Report Executive Summary," 24 April 1996. <http://www.mitre.org?research/y2k/docs/exec_sum.html>. 18 December 1996.

Shalikashvili, John M. Joint Vision 2010 . Washington, DC: The Joint Staff, 1996.

Spear, Ronald. "1 January 2000 is a Saturday," n.d. <http://www.army.mil/disc4/newslet/vp-96win/yr2000.htm>. 16 December 1996.

Starry, Donn A. and Huba Wass de Czege. "How To Change an Army." March 1983 and November 1984. <http://call.mil:1100/call/exfor/specrpt/exsum.htm>. 15 January 1997. 16. Analysis of the Toffler-Brown perspective indicates a need to add the factor of information to the eight "constants" of the Starry-Wass de Czege paradigm.

Steele, Robert D. "Creating A Smart Nation: Information Strategy, Virtual Intelligence and Information Warfare." Cyberwar: Securit, Strategy, and Conflict in the Information Age, ed. Alan Campen, Douglas Dearth, and R. Thomas Goodden (Fairfax, VA: AFCEA International Press, 1996.

Sullivan, Gordon. "Army Drawdown, An Army Chief of Staff Chain-Teaching Briefing on the Army Drawdown." Fort Bragg, NC, 1992.

Sullivan, Gordon R., and Michael V. Harper. Hope is Not a Method. New York: Times Books, 1996.

U.S. Congress, Senate, Subcommittee on Oversight of Government, Senate Government Affairs Committee. Computer Chaos: Billions Wasted Buying Federal Computer Systems. Report prepared by Senator William S. Cohen. 103d Cong., 2d sess., 1994. <http://ftp.senate.gov:70/0/member/me/cohen/general/computer_chaos>. 4 November 96.

U.S. Department of the Army. Information Operations. Field Manual No. 100-6. Washington: U.S. Department of the Army, 27 August 1996.

U.S. Department of Defense. Information Operations (IO) (U). Department of Defense Directive S-3600.1. Washington: U.S. Department of Defense, 9 December 1996.

U.S. General Accounting Office. HR-97-9 High-Risk Series. Information Management and Technology, February 1997. <http:/www.gao.gov/highrisk/hr97009.txt>. 13 February 1997.

U.S. General Accounting Office. Information Superhighway: An Overview of Technology Challenges. Washington: United States General Accounting Office, January 1995.

U.S. General Accounting Office. Information Technology Investment: Agencies Can Improve Performance, Reduce Costs, and Minimize Risks. Washington: U.S. General Accounting Office, 1996. <http://www.access.gpo.gov/cgi-bin/useftp....i96064.txt&directory=/diskb/wais/data/gao>. 2 November 1996.

U.S. General Accounting Office. Information Technology: Best Practices Can Improve Performance and Produce Results. Washington: U.S. General Accounting Office, 26 February 1996. <http://www.access.gpo.gov/cgi-bin/useftp....i96046.txt&directory=/diskb/wais/data/gao>.2 November 1996.

U.S. Office of Management and Budget. "Getting Federal Computers Ready for 2000," 6 February 1997. <http://www.comlinks.com/gov/omb2697.htm>. 21 February 1997.

U.S. Joint Staff. Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Joint Pub 6-0. Washington: U.S. Joint Staff, 30 May 1995.

U.S. Joint Staff. Doctrine for Joint Operations, Joint Publication 3-0. Washington: U.S. Joint Staff, 1 February 1995.

Valletta, Tony. "Year 2000 Problem," 2 May 1996. <http://www.itpolicy.gsa.gov/mks/yr2000/y220dmb2.htm>. 12 January, 1997.

White, John P. "Outsourcing Stretches DoD Dollars." Defense 96 (Issue 3): 21-23.

Willis, C. "PERSCOM to Remodel Personnel Information System Architecture," n.d. <http://www-prescom.army.mil/gendocs/strategic.htm>. 2 January 1997.

Wilkinson, Rod. "The T&E response to the 14 Nov DTSE&E memo (USD)(A&T) Year 2000 Kick-off Meeting) requiring an updated report of anticipated Year 2000 impacts for each functional user." 11 December 1996. < http://140.229.1.16:9000/htdocs/teinfo/y2kstat.htm>. 8 February 1997.

Woffinden, Duard S. "Artificial Intelligence and the Information Interoperability Puzzle." A paper for the 2nd International Workshop on Multimedia Information Systems. West Point, New York, 28 September 1996.